CERTIFICATE OF TRANSMISSION

I hereby certify that this correspondence (along with any paper referred to as being attached or enclosed) is being submitted *via* the USPTO EFS Filing System on the date shown below to **Mail Stop Appeal Brief - Patents**, Commissioner for Patents, P.O. Box 1450, Alexandria, Virginia 22313-1450.

Date: August 18, 2006 /Jessica Sexton/
Jessica Sexton

IN THE UNITED STATES PATENT AND TRADEMARK OFFICE

In re patent application of:			
Appellant(s):	Narayanan Ganapathy	Examiner:	Brandon S. Hoffman
Serial No:	09/772,231	Art Unit:	2136
Filing Date:	January 29, 2001		

Title: ISOLATION OF COMMUNICATION CONTEXTS TO FACILITATE COMMUNICATION OF DATA

Mail Stop Appeal Brief-Patents
Commissioner for Patents
P.O. Box 1450
Alexandria, VA 22313-1450

APPEAL BRIEF

Dear Sir:

Appellants submit this brief in connection with an appeal of the above-identified patent application. A credit card payment form is filed concurrently herewith in connection with all fees due regarding this appeal brief. In the event any additional fees may be due and/or are not covered by the credit card, the Commissioner is authorized to charge such fees to Deposit Account No. 50-1063 [MSFTP186US].

I. Real Party in Interest (37 C.F.R. §41.37(c)(1)(i))

The real party in interest in the present appeal is Microsoft Corporation, the assignee of the present application.

II. Related Appeals and Interferences (37 C.F.R. §41.37(c)(1)(ii))

Appellants, appellants' legal representative, and/or the assignee of the present application are not aware of any appeals or interferences which may be related to, will directly affect, or be directly affected by or have a bearing on the Board's decision in the pending appeal.

III. Status of Claims (37 C.F.R. §41.37(c)(1)(iii))

Claims 1-4 and 6-35 stand rejected by the Examiner. Claim 5 has been cancelled. The rejection of claims 1-4 and 6-35 is being appealed.

IV. Status of Amendments (37 C.F.R. §41.37(c)(1)(iv))

No amendments were made to claims after the Final Office Action dated March 17, 2006.

V. Summary of Claimed Subject Matter (37 C.F.R. §41.37(c)(1)(v))

A. Independent Claim 1

Independent claim 1 recites a system to facilitate secure communication of data from a user-level process, comprising: at least a first queue associated with a first process, such that the process is operative to directly communicate a message relative to the first queue; and a first communication context operative to communicate the message between the first queue and a second communication context; wherein communication between the first queue and the first communications context is controlled based on whether an appropriate association exists between the first queue and the first communications context, the association between the first queue and the first communications context being provided through a privileged operation not adjustable by the first process, the association between the first queue and the first communication context requires membership to a common domain.. (*See e.g.*, page 3, lines 5-30; page 5, line 27-page 6, line 6; page 7, lines 1-5; page 7, lines 15-17)

B. Independent Claim 14

Independent claim 14 recites a system to facilitate communication of data, comprising: a virtual hardware component at a first node operable to communicate a message received directly from an associated process; and a first channel endpoint established at the first node, the first channel endpoint being operative to communicate messages to a second channel endpoint residing at a second node; wherein each of the virtual hardware component and the first channel endpoint is associated with a respective domain through a privileged operation at the first node, communication of messages between the virtual hardware component and the first channel endpoint being controlled based on validation of the respective domains for the virtual hardware component and the first channel endpoint being a common domain.. (*See e.g.*, page 3, lines 5-30; page 5, line 27-page 6, line 6; page 7, lines 1-5; page 7, lines 15-17; page 14, line 27-page 15, line 12)

C. Independent Claim 22

Independent claim 22 recites a system to facilitate communication of data, comprising: storage means for receiving a message provided directly from a user-level process; communication means associated with the storage means for, upon validation of a common domain association between the storage means and the communication means, sending the stored request to a corresponding communication means at another node in the system; and validation means for validating the association between the storage means and the communication means, the storage means and the communication means being associated in a privileged operation not adjustable by user-level processes.. (*See e.g.*, page 3, lines 5-30; page 5, line 27-page 6, line 6; page 7, lines 1-5; page 7, lines 15-17)

D. Independent Claim 23

Independent claim 23 recites a system to facilitate communication of data, comprising:

virtual storage means at a first node for storing a message for direct communication relative to a user-level process; (*See e.g.*, page 6, lines 1-2; page 6, line 14; page 14, lines 20-24)

endpoint communication means at the first node for means for, upon determining a common domain membership for the storage means and the endpoint communication means,

enabling communication between the virtual storage means and the endpoint communication means; and (*See e.g.*, page 6, line 6; page 6, line 14; page 15, lines 13-16; page 15, lines 23-26)

control means for independently controlling domain membership for each of the virtual storage means and the endpoint communication means. (*See e.g.*, page 7, lines 4-5; page 14, line 28-page 15, line 1)

E. Independent Claim 26

Independent claim 26 recites a computer-readable medium having computer-executable instructions for: in a privileged mode, setting domain membership for a queue of a first node and setting domain membership for a communication component of the first node, the communication component of the first node being operable to communicate messages with a corresponding communication component at a second node, the domain membership being inaccessible by user-level processes, the queue being mapped into memory of an associated user-level process at the first node, such that the user-level process can communicate directly with the queue; and controlling communication of message between the queue and the communication component based on the domain membership set for each of the queue and the communication component being the same.. (*See e.g.*, page 3, lines 5-30; page 5, line 27-page 6, line 6; page 7, lines 1-5; page 7, lines 15-17)

F. Independent Claim 29

Independent claim 29 recites a method to facilitate communication in a system architecture in which a process is operative to communicate a message directly with a storage component coupled to at least one local communications component in a node for communicating the message for receipt by a second communications component, the method comprising: associating the storage component with a domain for temporarily storing the message; associating the local communications component with a domain; and controlling communication of a message between the storage component and the local communications component based on the domain of the storage component and the domain of the local communications component being identical. (*See e.g.*, page 3, lines 5-30; page 5, line 27-page 6, line 6; page 7, lines 1-5; page 7, lines 15-17)

VI. Grounds of Rejection to be Reviewed (37 C.F.R. §41.37(c)(1)(vi))

A. Whether claims 1-4 and 6-35 are unpatentable under 35 U.S.C. §102(b) over Tucker *et al.* (U.S. 5,808,911).

VII. Argument (37 C.F.R. §41.37(c)(1)(vii))

A. Rejection of Claims 1-4 and 6-35 Under 35 U.S.C. §102(b)

Claims 1-4 and 6-35 are rejected under 35 U.S.C. §102(b) as being anticipated by Tucker *et al.* (U.S. 5,808,911). It is respectfully submitted that this rejection should be withdrawn for at least the following reasons. Tucker *et al*. does not teach each and every element of the subject invention as recited in the subject claims.

> A single prior art reference anticipates a patent claim only if it expressly or inherently describes each and every limitation set forth in the patent claim. *Trintec Industries, Inc., v. Top-U.S.A. Corp.*, 295 F.3d 1292, 63 U.S.P.Q.2D 1597 (Fed. Cir. 2002); *See Verdegaal Bros. v. Union Oil Co. of California*, 814 F.2d 628, 631, 2 USPQ 2d 1051, 1053 (Fed. Cir. 1987). The identical invention must be shown in as complete detail as is contained in the … claim. *Richardson v. Suzuki Motor Co*., 868 F.2d 1226, 9 USPQ2d 1913, 1920 (Fed. Cir. 1989).

The subject invention relates to providing secure communication from a user-level application or process that has direct access to communication hardware components. The communication is secured by validating that a queue and a communication context that are to communicate with each other are part of the same domain. If they are not part of the same domain the system can prevent communication and report an error. Employing domains to secure access to communication contexts allows for tighter control over how many and which queues are communicating with a given communication context to better manage performance and prevent one process from taking a majority of the communication context bandwidth and starving use of the communication context from other processes. In particular, independent claim 1 (and similarly claims 14, 22, 23,26 and 29) recites *communication between the first queue and the first communications context is controlled based on whether an appropriate*

association exists between the first queue and the first communications context, the association between the first queue and the first communications context being provided through a privileged operation not adjustable by the first process, ***the association between the first queue and the first communication context requires membership to a common domain***.

Tucker *et al*. does not teach or suggest the aforementioned novel aspects of appellant's invention as recited in the subject claims. The cited art is concerned with management and cleanup of object references and discloses a method for tracking and counting object references at three levels; within the object's domain (handler level), in a different domain within the same node (door level), and that exist outside the node (xdoor level). Tucker *et al*. does not provide any suggestion for employing domains to secure access to objects. On the contrary, Tucker *et al*. explicitly states in column 3, lines 5-11, "Each thread can request the execution of an object (i.e., object's method). The location of the object is transparent to the thread. *The object can reside in one of several locations. It can reside within the same domain as the requesting thread, in a different domain as the requesting thread but within the same node as the requesting thread, or in the domain of a remote node*." The cited art clearly indicates that the thread and object are ***not required*** to reside within the same domain to communicate. Tucker *et al*. merely indicates that the object can reside in the same domain as the thread. Moreover, as disclosed in the above cited passage, Tucker *et al* discloses that the domains of the thread and object do not have to be the same and are not employed to secure access to the object. Appellant's claimed invention employs the domains of the queue and the communications context to control communication between them. In particular, as taught in the subject claims, communication between the queue and communication context is controlled based on their association indicating that they are in the same domain. Tucker *et al*. does not teach employing domains as a security mechanism for controlling communication between a queue and communication context. Furthermore, Tucker *et al*. states on column 4, lines 1-4, "The use of a file descriptor 154 to represent a door provides a secure mechanism to control the objects that a user can invoke. A file descriptor 154 is a protected kernel state and as such cannot be forged by a user. The possession of a file descriptor 154 indicates that an application has permissible access to an object." The cited art uses file descriptors associated with the object to secure access to the object. Applications that have a reference to a file descriptor can access the object associated with the file descriptor. Tucker *et al*. discloses that the applications and references to the file descriptor do not need to reside in the

same domain as the object associated with the file descriptor. Thus, Tucker *et al*. clearly does not disclose or suggest employing domains to secure communication. Therefore, Tucker *et al*. fails to teach or suggest that the association between the first queue and the first communication context requires membership to a common domain.

In view of the foregoing, appellant's representative respectfully submits that Tucker *et al* fails to teach or suggest all limitations of the subject invention as recited in independent claims 1, 14, 22, 23, 26 and 29 (and claims 2-4, 6-13, 15-21, 24, 25, 27, 28, and 30-35 that depend there from), and thus fails to anticipate the claimed invention. Accordingly, withdrawal of this rejection is respectfully requested.

CONCLUSION

The present application is believed to be in condition for allowance in view of the above comments and amendments. A prompt action to such end is earnestly solicited.

In the event any fees are due in connection with this document, the Commissioner is authorized to charge those fees to Deposit Account No. 50-1063 [MSFTP186US].

Should the Examiner believe a telephone interview would be helpful to expedite favorable prosecution, the Examiner is invited to contact appellant's undersigned representative at the telephone number below.

Respectfully submitted,
AMIN & TUROCY, LLP

/Himanshu S. Amin/
Himanshu S. Amin
Reg. No. 40,894

AMIN & TUROCY, LLP
24TH Floor, National City Center
1900 E. 9TH Street
Cleveland, Ohio 44114
Telephone (216) 696-8730
Facsimile (216) 696-8731

VIII. Claims Appendix (37 C.F.R. §41.37(c)(1)(viii))

1. A system to facilitate secure communication of data from a user-level process, comprising:

at least a first queue associated with a first process, such that the process is operative to directly communicate a message relative to the first queue; and

a first communication context operative to communicate the message between the first queue and a second communication context;

wherein communication between the first queue and the first communications context is controlled based on whether an appropriate association exists between the first queue and the first communications context, the association between the first queue and the first communications context being provided through a privileged operation not adjustable by the first process, the association between the first queue and the first communication context requires membership to a common domain.

2. The system of claim 1, wherein the first queue and the first communication context reside at a first node that is different from that of the second communication context.

3. The system of claim 2, further comprising an interface at the first node operative to validate messages communicated from the first queue to the first communication context.

4. The system of claim 3, wherein the interface is operative to prevent messages from being communicated from the first queue to the first communication context if an association mismatch exists between the first queue and the first communication context.

5. (Cancelled)

6. The system of claim 2, further comprising a second queue associated with a second process at the first node, such that the second process is operative to directly communicate a message to the second queue.

7. The system of claim 6, wherein the second queue is associated with the common domain through a privileged operation, such that the first and second queues can share the first communication context to communicate messages through a channel defined by the first communication context and the second communication context, each of the first and second queues being operative to communicate messages with at least one process at a node where the second communication context resides.

8. The system of claim 7, wherein the first process further comprises a process operating in a user mode and the second process comprises a process operating in a user mode.

9. The system of claim 6, further including a third communication context associated with the second queue through a privileged operation at the first node, the third communication context enabling communication between the third communication context and a fourth communication context that resides a node different from the first node.

10. The system of claim 9, wherein the common domain is a first domain, the association between the second queue and the third communication context corresponding to a second domain that is different from the first domain, wherein each communication channel established in the second domain is isolated from each channel established in the first domain.

11. The system of claim 1, wherein the first queue and the first communication context reside at a first node that is different from a second node at which the second communication context resides, the system further comprising a third communication context at the first node to enable communication of messages between the third communication context and a fourth communication context that resides at a third node that is different from the first node.

12. The system of claim 11, wherein the first queue is associated with the third communication context through a privileged operation, such that the first process is operative to communicate the message over a communication channel established between the third communication context and a fourth communication context that resides at the third node, which is different from the second node.

13. The system of claim 11, wherein the first queue and the first communication context are associated so as to be part of a first domain, the system further comprising a second queue is associated with a second process, the second queue being associated with a third communication context so as to be part of second domain that is isolated relative to the first domain.

14. A system to facilitate communication of data, comprising:

a virtual hardware component at a first node operable to communicate a message received directly from an associated process; and

a first channel endpoint established at the first node, the first channel endpoint being operative to communicate messages to a second channel endpoint residing at a second node;

wherein each of the virtual hardware component and the first channel endpoint is associated with a respective domain through a privileged operation at the first node, communication of messages between the virtual hardware component and the first channel endpoint being controlled based on validation of the respective domains for the virtual hardware component and the first channel endpoint being a common domain.

15. The system of claim 14, wherein hardware at the first node is operative to prevent messages from being sent between the virtual component and the first channel endpoint in response to detecting an invalid association between the virtual hardware component and the first channel endpoint.

16. The system of claim 14, wherein the virtual hardware component is a first virtual component, the system further comprising a second virtual hardware component operative to communicate a message directly with an associated process at the first node.

17. The system of claim 16, wherein the second virtual hardware component and the first virtual hardware component are members of a common domain, domain membership being assigned through a privileged operation not adjustable by the first or second process, wherein the first and second virtual hardware components are operative to share the first channel endpoint of

the first node, such that each of the first and second processes can communicate messages with at least one process at the second node.

18. The system of claim 14, further including a third channel endpoint at the first node, the third channel endpoint being operative to communicate messages with a fourth channel endpoint that resides at a node different from the first node.

19. The system of claim 18, wherein the virtual hardware component is a first virtual hardware component, the system further comprising a second virtual hardware component at the first node that is associated with the third channel endpoint through a privileged operation at the first node.

20. The system of claim 19, wherein each of the first and third channel endpoints belongs to different domains, such that each communication channel established between associated channel endpoints in one of the domains is isolated from each communication channel established between associated channel endpoints in each other of the domains.

21. The system of claim 19, wherein each of the first and third channel endpoints belongs to a common domain, such that each of the first and second processes at the first node is operative to share first and third channel endpoints to respectively communicate a message with at least one process at the second and third nodes based on data in the respective message.

22. A system to facilitate communication of data, comprising:

storage means for receiving a message provided directly from a user-level process;

communication means associated with the storage means for, upon validation of a common domain association between the storage means and the communication means, sending the stored request to a corresponding communication means at another node in the system; and

validation means for validating the association between the storage means and the communication means, the storage means and the communication means being associated in a privileged operation not adjustable by user-level processes.

23. A system to facilitate communication of data, comprising:

virtual storage means at a first node for storing a message for direct communication relative to a user-level process;

endpoint communication means at the first node for means for, upon determining a common domain membership for the storage means and the endpoint communication means, enabling communication between the virtual storage means and the endpoint communication means; and

control means for independently controlling domain membership for each of the virtual storage means and the endpoint communication means.

24. The system of claim 23, wherein the endpoint communication means further includes means for preventing communication of messages between the virtual storage means and the endpoint communication means in the absence of a common domain membership among virtual storage means and the endpoint communication means.

25. The system of claim 23, wherein the endpoint communication means further includes means for permitting communication of messages between the virtual storage means and the endpoint communication means when common domain membership exists among virtual storage means and the endpoint communication means.

26. A computer-readable medium having computer-executable instructions for:

in a privileged mode, setting domain membership for a queue of a first node and setting domain membership for a communication component of the first node, the communication component of the first node being operable to communicate messages with a corresponding communication component at a second node, the domain membership being inaccessible by user-level processes, the queue being mapped into memory of an associated user-level process at the first node, such that the user-level process can communicate directly with the queue; and

controlling communication of message between the queue and the communication component based on the domain membership set for each of the queue and the communication component being the same.

27. The computer-readable medium of claim 26 having further computer-executable instructions for providing an error message to the associated user-level process if the domain membership between the queue and the communication component is invalid.

28. The computer-readable medium of claim 26 having further computer-executable instructions for analyzing the message to identify which of a plurality of communication contexts is designated and validating domain membership between the queue and the designated communication context to control communication of the message between the queue and the designated communication context.

29. A method to facilitate communication in a system architecture in which a process is operative to communicate a message directly with a storage component coupled to at least one local communications component in a node for communicating the message for receipt by a second communications component, the method comprising:

associating the storage component with a domain for temporarily storing the message;

associating the local communications component with a domain; and

controlling communication of a message between the storage component and the local communications component based on the domain of the storage component and the domain of the local communications component being identical.

30. The method of claim 29, wherein the domain for the storage component and the domain for the association of the local communications component are implemented independently in privileged operation not adjustable by the user-level process.

31. The method of claim 30, wherein the controlling further comprises validating the domain of the storage component relative the domain of the local communication component.

32. The method of claim 31, further comprising preventing communication of the message from the storage component to the communication component in the absence of a match between the domain of the storage component and the domain of the communication component.

33. The method of claim 32, further comprising generating an error message in the absence of a match between the domain of the at least part of the storage component and the domain of the communication component.

34. The method of claim 32, further comprising sending the message from the storage component to the communication component in response to a valid association existing between the domain of the storage component and the domain of the communication component.

35. The method of claim 30, further comprising discerning from the message which of at least one of a plurality of communication components is designated and validating association between the storage component and each designated communication component to control communication of the message between the storage component and each designated communication component.

IX. Evidence Appendix (37 C.F.R. §41.37(c)(1)(ix))

None.

X. Related Proceedings Appendix (37 C.F.R. §41.37(c)(1)(x))

None.